

DT05 Rec 5 CT/PTO 10 DEC 2003

DOCKET NO.: 263082US90XPCT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Ken SAKAMURA et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/JP03/07250

INTERNATIONAL FILING DATE: June 9, 2003

FOR: IC CARD, TERMINAL DEVICE, AND DATA COMMUNICATION METHOD

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119  
AND THE INTERNATIONAL CONVENTION**Commissioner for Patents  
Alexandria, Virginia 22313

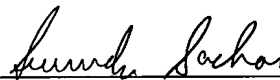
Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<b><u>COUNTRY</u></b>	<b><u>APPLICATION NO</u></b>	<b><u>DAY/MONTH/YEAR</u></b>
Japan	2002-169241	10 June 2002
Japan	2002-169244	10 June 2002

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP03/07250.

Respectfully submitted,  
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Masayasu Mori  
Attorney of Record  
Registration No. 47,301  
Surinder Sachar  
Registration No. 34,423

Customer Number

**22850**

(703) 413-3000  
Fax No. (703) 413-2220  
(OSMMN 08/03)

Rec'd PCT/PTO 10 DEC 2004

10/516309

日本国特許庁  
JAPAN PATENT OFFICE

PCT/JP 03/07250

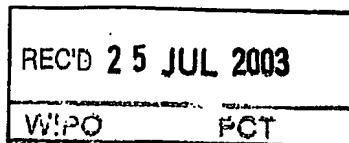
09.06.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2002年 6月10日

出願番号  
Application Number: 特願2002-169241  
[ST. 10/C]: [JP 2002-169241]



出願人  
Applicant(s):

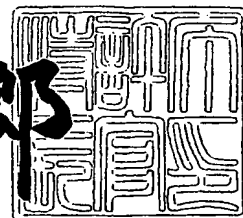
坂村 健  
越塚 登  
株式会社エヌ・ティ・ティ・ドコモ

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2003年 7月 9日

特許庁長官  
Commissioner,  
Japan Patent Office

太田信一郎



【書類名】 特許願

【整理番号】 DCMH130666

【提出日】 平成14年 6月10日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明の名称】 ICカード、端末装置及びデータ交換方法

【請求項の数】 16

【発明者】

    【住所又は居所】 東京都品川区大崎4-9-2

    【氏名】 坂村 健

【発明者】

    【住所又は居所】 東京都武蔵野市西久保2-27-20

    【氏名】 越塚 登

【発明者】

    【住所又は居所】 東京都千代田区永田町二丁目11番1号 株式会社エヌ・ティ・ティ・ドコモ内

    【氏名】 森 謙作

【発明者】

    【住所又は居所】 東京都千代田区永田町二丁目11番1号 株式会社エヌ・ティ・ティ・ドコモ内

    【氏名】 石井 一彦

【発明者】

    【住所又は居所】 東京都千代田区永田町二丁目11番1号 株式会社エヌ・ティ・ティ・ドコモ内

    【氏名】 青野 博

【発明者】

    【住所又は居所】 東京都千代田区永田町二丁目11番1号 株式会社エヌ・ティ・ティ・ドコモ内

    【氏名】 本郷 節之

## 【特許出願人】

【識別番号】 592146793

【氏名又は名称】 坂村 健

## 【特許出願人】

【住所又は居所】 東京都武蔵野市西久保 2-27-20

【氏名又は名称】 越塚 登

## 【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社 エヌ・ティ・ティ・ドコモ

## 【代理人】

【識別番号】 100083806

## 【弁理士】

【氏名又は名称】 三好 秀和

【電話番号】 03-3504-3075

## 【選任した代理人】

【識別番号】 100100712

## 【弁理士】

【氏名又は名称】 岩▲崎▼ 幸邦

## 【選任した代理人】

【識別番号】 100095500

## 【弁理士】

【氏名又は名称】 伊藤 正和

## 【選任した代理人】

【識別番号】 100101247

## 【弁理士】

【氏名又は名称】 高橋 俊一

## 【手数料の表示】

【予納台帳番号】 001982

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9702416

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ICカード、端末装置及びデータ交換方法

【特許請求の範囲】

【請求項 1】 デジタルコンテンツを格納するホルダー部と、

前記ホルダー部に格納されたデジタルコンテンツに対応付けられた鍵情報を含む証明書データを格納する証明書記憶部と、

前記ホルダー部に格納されたデジタルコンテンツを、前記鍵情報に基づいて暗号化する暗号処理部と、

暗号化されたデジタルコンテンツを、他の機器に対して送信するとともに、該他の機器が保持するデジタルコンテンツを受信するデータ送受信部と、

前記ホルダー部に格納されたデジタルコンテンツを前記暗号処理部により暗号化し、これを前記データ送信部を通じて送信するとともに、前記他の機器からデジタルコンテンツを受信するためのコマンドを記憶するコマンド記憶部と、

外部からのトリガー信号に基づいて、前記コマンドを実行する実行処理部とを備え、

前記コマンドは、

前記デジタルコンテンツの送信前における各部の状態を記憶させ、

前記デジタルコンテンツの送信後、送信先が受信処理を完了した旨を通知するコミット命令を受信し、

前記コミット命令に応じて、前記他の機器に対してデジタルコンテンツの送信を要求する送信要求を送信し、

前記送信要求に応じて送信されたデジタルコンテンツの受信が完了した場合に、その旨を通知する送信完了通知を送信し、

前記ホルダー部内に格納されたデジタルコンテンツを消去し、

デジタルコンテンツの送信処理が中断された場合には、記憶された状態に各部を復帰させる

ことを特徴とする ICカード。

【請求項 2】 前記証明書データには、前記ホルダー部を識別するホルダー ID 及び、当該証明書情報を発行した者が該証明書情報が正当である旨を保証す

る署名データとが含まれ、

前記デジタルコンテンツの送信に先だって、送信先から該送信先の証明書データを取得し、取得した証明書データに含まれる送信先のホルダーID及び署名データとにより当該送信先の正当性を認証する認証部を有し、

前記実行処理部は、前記送信先が正当であると認証された場合に、前記コマンドを実行することを特徴とする請求項1に記載のICカード。

【請求項3】 前記認証部は、認証の際に、現在、確立されている通信を識別するセッションIDと、指定されたセッションモードを取得し、取得されたセッションIDとセッションモードに応じて、前記ホルダ部に格納されているデジタルコンテンツへのアクセスレベルを設定することを特徴とする請求項2に記載のICカード。

【請求項4】 前記証明書データには、前記ホルダー部を識別するホルダーID及び、当該証明書情報を発行した者が該証明書情報が正当である旨を保証する署名データとが含まれ、

前記デジタルコンテンツの送信に先だって、送信先に対して当該ICカード側の証明書データを送信し、送信側から、当該証明書情報の正当性が認証された旨を通知する認証確認通知を取得する認証部を有し、

前記実行処理部は、前記認証確認通知が取得された場合に、前記コマンドを実行することを特徴とする請求項1乃至3のいずれかに記載のICカード。

【請求項5】 前記コマンドは、

前記デジタルコンテンツの送信前における送信先の状態を記憶させ、

デジタルコンテンツの交換処理が中断された場合に、前記送信先の状態を記憶された状態に復帰させる

ことを特徴とする請求項1乃至4のいずれかに記載のICカード。

【請求項6】 請求項1に記載のICカードに記憶された前記デジタルコンテンツを送信する端末装置であって、

操作信号を入力する操作部と、

前記操作信号に基づいて、前記コマンドの実行処理を開始させるトリガー信号を前記実行処理部に対して出力する制御部と

を有することを特徴とする端末装置。

【請求項 7】 前記通信部による通信状態を監視する通信監視部を備え、  
該通信監視部は、最後にデータを送信した時点からの経過時間を測定し、所定の待機時間を経過するまでの間に送信先からの応答がない場合に、通信が中断された旨を前記実行処理部に送出することを特徴とする請求項 6 に記載の端末装置。

【請求項 8】 現在、確立されている通信を識別するセッション ID と、指定されたセッションモードとに応じて設定された、前記デジタルコンテンツへのアクセスレベルに基づいて、当該デジタルコンテンツに関する情報を前記ホルダー部から読み出し、表示する表示部を有することを特徴とする請求項 6 又は 7 に記載の端末装置。

【請求項 9】 IC カード内に蓄積されたデジタルコンテンツ他の端末装置内に蓄積されたデジタルコンテンツと交換するデータ交換方法であって、

IC カード内に前記デジタルコンテンツを格納するとともに、この格納されたデジタルコンテンツに対応付けられた鍵情報を含む証明書データを前記 IC カード内に格納し、さらに、前記デジタルコンテンツの暗号化及び送信を行うためのコマンドを IC カード内に記憶するコマンド記憶部に記憶するステップ(1)と、

外部からのトリガー信号に基づいて、前記コマンドを実行し、前記デジタルコンテンツを、前記鍵情報に基づいて暗号化するとともに、暗号化されたデジタルコンテンツを、外部に対して送信するステップ(2)とを有し、

前記ステップ(2)においては、

前記デジタルコンテンツの送信前における各部の状態を記憶させ、

前記デジタルコンテンツの送信後、送信先が受信処理を完了した旨を通知するコミット命令を受信し、

前記コミット命令に応じて、前記他の機器に対してデジタルコンテンツの送信を要求する送信要求を送信し、

前記送信要求に応じて送信されたデジタルコンテンツの受信が完了した場合に、その旨を通知する送信完了通知を送信し、

前記ホルダー部内に格納されたデジタルコンテンツを消去し、デジタルコンテ



ンツの送信処理が中断された場合には、記憶された状態に各部を復帰させることを特徴とするデータ交換方法。

【請求項 10】 前記証明書データには、前記ホルダー部を識別するホルダー ID 及び、当該証明書情報を発行した者が該証明書情報が正当である旨を保証する署名データとが含まれ、

前記ステップ(2)におけるデジタルコンテンツの送信に先だって、

送信先から該送信先の証明書データを取得し、取得した証明書データに含まれる送信先のホルダー ID 及び署名データとにより当該送信先の正当性を認証し、

前記送信先が正当であると認証された場合に、前記コマンドを実行することを特徴とする請求項 9 に記載のデータ交換方法。

【請求項 11】 前記認証の際に、現在、確立されている通信を識別するセッション ID と、指定されたセッションモードを取得し、取得されたセッション ID とセッションモードに応じて、前記ホルダー部に格納されているデジタルコンテンツへのアクセスレベルを設定することを特徴とする請求項 10 に記載のデータ交換方法。

【請求項 12】 前記証明書データには、前記ホルダー部を識別するホルダー ID 及び、当該証明書情報を発行した者が該証明書情報が正当である旨を保証する署名データとが含まれ、

前記ステップ(2)におけるデジタルコンテンツの送信に先だって、

送信先に対して当該 IC カード側の証明書データを送信し、送信側から、当該証明書情報の正当性が認証された旨を通知する認証確認通知を取得し、

前記実行処理部は、前記認証確認通知が取得された場合に、前記コマンドを実行することを特徴とする請求項 9 乃至 11 のいずれかに記載のデータ交換方法。

【請求項 13】 前記コマンドは、

前記デジタルコンテンツの送信前における送信先の状態を記憶させ、

デジタルコンテンツの送信処理が中断された場合に、前記送信先の状態を記憶された状態に復帰させる

ことを特徴とする請求項 9 乃至 12 のいずれかに記載のデータ交換方法。

【請求項 14】 前記 IC カードは端末装置内装填され、

端末装置の操作部から操作信号を入力するステップ(3)と、  
前記操作信号に基づいて、前記コマンドの実行処理を開始させるトリガー信号を前記実行処理部に対して出力するステップ(4)と  
を有することを特徴とするデータ交換方法。

【請求項 15】 前記端末装置において、他の通信機器との通信状態を監視するステップと、

最後にデータを送信した時点からの経過時間を測定し、所定の待機時間を経過するまでの間に送信先からの応答がない場合に、通信が中断された旨を I C カードに対して送出することを特徴とする請求項 14 に記載のデータ交換方法。

【請求項 16】 現在、確立されている通信を識別するセッション I D と、指定されたセッションモードとに応じて、前記デジタルコンテンツへのアクセスレベルを設定し、

当該デジタルコンテンツに関する情報を I C カードから読み出し、表示することを特徴とする請求項 14 又は 15 に記載のデータ交換方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、e コマースやコンテンツ配信等に利用可能なデジタルコンテンツを、I C カードと他の端末装置間で交換する機能を有する I C カード、及びこの I C カードを操作するための端末装置、及び前記デジタルコンテンツの交換方法に関する。

【0002】

【従来の技術】

従来より、電子マネー等のデジタルコンテンツを I C カード内に格納し、このデジタルコンテンツをリーダライタ等の操作端末装置で読み出し、これを送信先の装置へ送信するとともに、他の端末装置に格納されたデジタルコンテンツを受信することによって、デジタルコンテンツを交換する通信プラットフォームが開発されている。

【0003】

従来のプラットフォームでは、操作端末装置においてＩＣカードからデジタルコンテンツを読み出し、操作端末装置に備えられたハードウェアやソフトウェアのコマンドにより暗号化処理を行うとともに、操作端末装置上で実行されているＯＳのプロトコルに基づいて、データの送受信を行っている。

#### 【０００４】

この送受信にあつては、データの安全な送信を担保するために、送信先に一時的に複製した後に、送信元のデジタルコンテンツを消去する方式を採用している。

#### 【０００５】

##### 【発明が解決しようとする課題】

しかしながら、上述した従来のシステムでは、ＩＣカード内に格納されたデジタルコンテンツを操作端末上に読み出し、操作端末側のコマンドやプロトコルにより処理がなされているため、操作端末側にデジタルコンテンツを読み出した際に、悪意の操作者や、悪意の第三者によってデジタルコンテンツの内容が改ざんされたり、不正に複製されたりする可能性があった。

#### 【０００６】

また、従来では、複数の操作端末装置間でデジタルコンテンツの送受信を行う場合、送信先に一時的に複製した後に、送信元のデジタルコンテンツを消去する方式を採用しているため、送受信処理中に通信が切断されたときには、送受信処理にかかるデジタルコンテンツが消失したり、或いは、送信先及び送信元の両方にデジタルコンテンツが存在する状態で処理が中断されることがあり、この場合には、操作者の意図によらず、デジタルコンテンツが複製される結果となる。

#### 【０００７】

特に、電子マネーなどによる取引においては、デジタルコンテンツが確実に交換されるか、或いは、通信障害が生じた場合には、取引開始時の状態に完全に復帰させる必要がある。

#### 【０００８】

本発明は、上記課題に鑑みてなされたものであり、ＩＣカード及び他の端末装置間で直接通信を行うプラットフォーム上で、デジタルコンテンツを交換する際に

、送受信者及び悪意のある第三者による複製や紛失を回避することのできる IC カード、端末装置、及びデータ交換方法を提供することを目的とする。

#### 【0009】

##### 【課題を解決するための手段】

上記課題を解決するために、本発明は、IC カード内に蓄積されたデジタルコンテンツ他の端末装置内に蓄積されたデジタルコンテンツと交換するデータ交換する際、IC カード内にデジタルコンテンツを格納するとともに、この格納されたデジタルコンテンツに対応付けられた鍵情報を含む証明書データを IC カード内に格納し、さらに、デジタルコンテンツの暗号化及び送信を行うためのコマンドを IC カード内に記憶するコマンド記憶部に記憶し、外部からのトリガー信号に基づいて、コマンドを実行し、デジタルコンテンツを鍵情報に基づいて暗号化するとともに、暗号化されたデジタルコンテンツを外部に対して送信し、送信側でデジタルコンテンツの送信前における各部の状態を記憶させ、デジタルコンテンツの送信後、送信先が受信処理を完了した旨を通知するコミット命令を受信し、コミット命令に応じて、他の機器に対してデジタルコンテンツの送信を要求する送信要求を送信し、送信要求に応じて送信されたデジタルコンテンツの受信が完了した場合に、その旨を通知する送信完了通知を送信し、ホルダー部内に格納されたデジタルコンテンツを消去し、デジタルコンテンツの送信処理が中断された場合には、記憶された状態に各部を復帰させる。

#### 【0010】

上記発明においては、証明書データには、ホルダー部を識別するホルダー ID 及び、証明書情報を発行した者が証明書情報が正当である旨を保証する署名データとが含まれ、デジタルコンテンツの交換に先だって、送信先から送信先の証明書データを取得し、取得した証明書データに含まれる送信先のホルダー ID 及び署名データとにより送信先の正当性を認証し、送信先が正当であると認証された場合に、コマンドを実行することが好ましい。

#### 【0011】

上記発明においては、認証の際に、現在、確立されている通信を識別するセッション ID と、指定されたセッションモードを取得し、取得されたセッション I

Dとセッションモードに応じて、ホルダ部に格納されているデジタルコンテンツへのアクセスレベルを設定することが好ましい。

#### 【0012】

上記発明においては、証明書データには、ホルダー部を識別するホルダーID及び、証明書情報を発行した者が証明書情報が正当である旨を保証する署名データが含まれ、デジタルコンテンツの送信に先だって、送信先に対してICカード側の証明書データを送信し、送信側から、証明書情報の正当性が認証された旨を通知する認証確認通知を取得し、実行処理部は、認証確認通知が取得された場合に、コマンドを実行することが好ましい。

#### 【0013】

上記発明においては、コマンドは、デジタルコンテンツの送信前における送信先の状態を記憶させ、デジタルコンテンツの送信処理が中断された場合に、送信先の状態を記憶された状態に復帰させることが好ましい。

#### 【0014】

上記発明においては、ICカードは端末装置内装填され、端末装置の操作部から操作信号を入力し、操作信号に基づいて、コマンドの実行処理を開始させるトリガー信号を実行処理部に対して出力することが好ましい。

#### 【0015】

上記発明においては、端末装置において、他の通信機器との通信状態を監視するステップと、最後にデータを送信した時点からの経過時間を測定し、所定の待機時間を経過するまでの間に送信先からの応答がない場合に、通信が中断された旨をICカードに対して送出することが好ましい。

#### 【0016】

上記発明においては、現在、確立されている通信を識別するセッションIDと、指定されたセッションモードとに応じて、デジタルコンテンツへのアクセスレベルを設定し、デジタルコンテンツに関する情報をICカードから読み出し、表示することが好ましい。

#### 【0017】

上記発明によれば、外部の端末装置やサーバのコマンドを用いることなく、I

Cカード内部に備えられたアトミックなコマンドを用いて暗号化や送信処理を行うことから、外部の端末装置やサーバ側からの不正な操作による影響を回避することができ、外部の装置のセキュリティー環境によらず、安全なデジタルコンテンツの送信を行うことができる。

#### 【0018】

また、デジタルコンテンツは、ICカード内で暗号化されるため、通信時にあつては、受信側の端末装置の操作者のみならず、送信側の端末装置の操作者であっても、デジタルコンテンツの内容を知ることができず、データの改ざんや複製を防止することができる。この結果、例えば監視サーバ等の第三者の監視を用いることなく、ICカード間で安全なデジタルコンテンツの送信が可能となる。

#### 【0019】

##### 【発明の実施の形態】

##### 〔第1実施形態〕

##### （データ交換システムの構成）

本発明のデータ交換システムの第1実施形態について図を参照しながら説明する図1は、本実施形態に係るデータ交換システムの構成を示す説明図である。図1に示すように、本実施形態では、機能分散システム上において、送信元であるICカード1aに格納されたデジタルコンテンツを、送信先であるICカード1bに対して送信する場合を例に説明する。図1に示すように、ICカード1a及び1bは、それぞれICチップ11a及び11bを搭載しているとともに、端末装置2a及び2bに装填され、各端末装置からの操作に基づいて、端末装置を介して、データの送受信を行う。

#### 【0020】

図2は、ICカード1a（1b）及び端末装置2a（2b）の内部構成を示すブロック図である。図2に示すように、ICカード1a（1b）は、それぞれに搭載されたICチップ11a（11b）と、ICチップ内のデータを端末装置2a（2b）に対して送受信するデータ送受信部12を備えている。

#### 【0021】

ICカード1a（1b）は、本実施形態においては、コンピュータの周辺機器

として、リーダライタを通して操作されるものではなく、分散環境におけるノードとして設計されており、ネットワーク上のサービス提供モジュールのチップに対して、対等にpeer-to-peer で通信が可能となっている。

#### 【0022】

ICチップ11a(11b)は、耐タンパ性を有するLSIであり、演算処理デバイスやメモリ等から構成され、ICカードの他、例えばスマートカード、携帯型端末といったハードウェア上に実装される。

#### 【0023】

端末装置2a(2b)は、ICカード1a(1b)が挿抜可能に装填され、ICカード1a(1b)に対してデータの読込及び書き込みを行うリーダライタ機能を備え、LAN等の通信ネットワークに対する、コンタクトレス通信の物理層を橋渡しするゲートウェイ(ブリッジ)の役割を果たすものである。具体的にこの端末装置2は、例えば、PDAや携帯電話等の形態を採ることができる。

#### 【0024】

(ICカードの構成)

ICチップ11a(11b)は、プラスチック等で形成されたカード基板上に固着された集積回路であり、具体的には、認証部13と、暗号処理部14と、実行処理部15と、コマンド記憶部16と、証明書データ格納部17と、ホルダー部18とを備えている。

#### 【0025】

認証部13は、他のICカードとの通信を確立する際に、他のICカードとの間で相互認証を行う演算デバイスである。具体的には、デジタルコンテンツの送信に先だって、送信先のICカードから送信先の証明書データを取得し、取得した証明書データに含まれる送信先のホルダーID及び署名データとにより当該送信先の正当性を認証するとともに、送信先に対して自機側の証明書データを送信し、送信側から、当該証明書情報の正当性が認証された旨を通知する認証確認通知を取得することによって、相互認証を行う。

#### 【0026】

また、本実施形態において、この認証部13は、認証の際に、現在、確立され

ている通信を識別するセッションIDと、指定されたセッションモードを取得し、取得されたセッションIDとセッションモードに応じて、ホルダー部18に格納されているデジタルコンテンツへのアクセスレベルを設定する。

#### 【0027】

このアクセスレベルは、本実施形態では、(情報)発行者モードと所有者モードのモードがあり、認証時に指定され、各モードによって認証アルゴリズムが異なる。

#### 【0028】

本実施形態に係るアクセスレベルは以下のものがある。

#### 【0029】

##### (1)(情報)発行者モード：

アクセス者を、デジタルコンテンツの発行者として認証するモードであり、発行者のモードで認証された後は、その情報提供者が作成したデジタルコンテンツには、発行者権限でアクセスでき、それ以外のデジタルコンテンツには、その他権限でアクセスすることができる。

#### 【0030】

##### (2)所有者モード：

アクセス者をチップの所有者として認証するモードであり、本実施形態では、パスワード等、人間にとって扱いやすい認証方法が使用される。所有者モードで認証されたアクセス者は所有者権限を持つ。

#### 【0031】

前記暗号処理部14は、ホルダー部18に格納されたデジタルコンテンツを、ICカード内部において、暗号化するものであり、ホルダー部18に格納されたデジタルコンテンツは、この暗号処理部14で暗号化された後、データ送受信部12を通じて端末装置側に送出される。

#### 【0032】

実行処理部15は、外部からのトリガー信号に基づいて、コマンド記憶部16からコマンドを呼び出し、デジタルコンテンツの暗号化や送信処理を実行する演算処理装置である。このトリガー信号は、本実施形態では、操作部24からの操



作信号に基づいて、制御部 26 が出力する。

【0033】

また、この実行処理部 15 は、認証部 13 と連動する形態となっており、認証部 13 で送信先の IC カードが正当であると認証されるとともに、送信先の IC カードの認証確認通知が取得され、相互認証が確立された場合に、前記コマンドを実行する。

【0034】

コマンド記憶部 16 は、ホルダー部 18 に格納されたデジタルコンテンツを暗号処理部 14 により暗号化したり、データ送受信部 12 を通じて送信したりするためのコマンドを記憶するメモリ等の記憶装置である。

【0035】

証明書データ格納部 17 は、ホルダー部 18 に格納されたデジタルコンテンツに対応付けられた証明書データを格納するメモリ等の記憶装置であり、認証部 13 における認証処理時や、暗号処理部 14 における暗号化処理時に、必要なデータであるホルダー ID や、鍵情報、署名データを読み出す。この証明書データの内容については、後述する。

【0036】

ホルダー部 18 は、他の IC カード等との間で、情報交換をするネットワーク上の計算実体であり、デジタルコンテンツを格納する耐タンパ性のメモリ装置である。

【0037】

データ送受信部 12 は、証明書データや暗号化されたデジタルコンテンツを、外部に対して送信する通信デバイスであり、接触式或いは非接触式によりデータを送受信する。なお、本実施形態におけるデータ送受信部 12 は、IC カード 1 が端末装置 2 内に装填された状態で、端末装置 2 側のデータ送受信部 23 と接触され、データの送受信を行うように形成されている。

【0038】

(操作端末の構成)

本実施形態に係る端末装置 2a (2b) は、カードリーダーや携帯電話、PDA

等の携帯端末装置、或いはパーソナルコンピュータ等の汎用コンピュータで実現することが可能であり、具体的には、図2に示すように、通信部21と、通信監視部22と、データ送受信部23と、操作部24と、表示部25と、制御部26とを備えている。

#### 【0039】

通信部21は、無線通信等により、データの送受信を行う通信デバイスである。通信監視部22は、通信部21による通信状態を監視する装置であり、最後にデータを送信した時点からの経過時間を測定し、所定の待機時間を経過するまでの間に送信先からの応答がない場合に、通信が中断されたと判断し、その旨をデータ送受信部23及び12を介して、ICカード内の実行処理部15に送出する。

#### 【0040】

データ送受信部23は、端末装置2内に装填されたICカードのデータ送受信部12と接触されるように設けられており、データ送受信部12との間でデータの送受信を行う。

#### 【0041】

操作部24は、例えば端末装置2の表面に配置されたボタンやスティックであり、操作者の操作により、種々の操作信号を制御部26に対して入力する操作デバイスである。

#### 【0042】

表示部25は、例えば端末装置2の表面に配置された液晶ディスプレイ等の表示デバイスであり、通信部21における通信状態や、操作部24における捜査結果を表示する。特に、本実施形態において、表示部25は、現在、他のICカードとの間で確立されている通信（セッション）を識別するセッションIDと、指定されたセッションモードとに応じて設定されたアクセスレベルに基づいて、当該デジタルコンテンツに関する情報をホルダー部から読み出し、表示する機能を有する。

#### 【0043】

制御部26は、端末装置2の各部21～25の動作を制御するCPUであり、

特に、操作部 24 からの操作信号に基づいて、実行処理部 15 におけるコマンドの実行処理を開始させるトリガー信号を実行処理部 15 に対して出力する。

#### 【0044】

(デジタルコンテンツ)

ICカードには、デジタルコンテンツを格納する多様なアプリケーションが実装される可能性があるため、デジタルコンテンツとしては、様々なタイプがあり、例えば、以下のようなものが考えられる。

#### 【0045】

- ・チップの所有者は変更できずに情報の発行者だけが変更できる情報（例：電子チケットの座席番号）
- ・チップの所有者でさえ見せない情報（例：電子チケット変更の鍵）
- ・チップの所有者だけが完全に制御できる情報（例：所有者の個人情報）
- ・読みことはだれでもできる情報

なお、このデジタルコンテンツは、発行サーバ等の第三者機関により発行され、証明書データとともに IC カード内に格納される。

#### 【0046】

(証明書データ)

前記証明書データには、ホルダー部 18 に格納されたデジタルコンテンツを識別するホルダー ID 及び証明書情報を発行した者が当該証明書情報が正当である旨を保証する署名データと、デジタルコンテンツに関連付けられた公開鍵情報が含まれている。

#### 【0047】

ホルダー ID は、分散システム全体でユニークに定められた識別子であり、IC カードを物理的に識別するだけでなく、分散環境上での経路制御にも利用され、認証通信における相手に対する識別子として利用される。すなわち、ホルダー ID は、ネットワーク上で、IC カードやサービスクライアントの認証、メッセージの経路制御などに用いられる。なお、本実施形態において、ホルダー ID は、16 オクテット (128 ビット) 数で表現される。

#### 【0048】

(コマンド)

前記コマンド記憶部 16 に格納されたコマンドは、端末装置 2 側からのトリガー信号が受信され、実行が開始されると、端末装置 2 側における操作とは独立してアトミックに一連の処理が進行される原子性を有するものである。

【0049】

このコマンドによる一連の処理としては、

- (1) 認証処理
- (2) 暗号化処理
- (3) 交換処理
- (4) 送信完了確認処理
- (5) デジタルコンテンツの消去処理

がある。

【0050】

すなわち、コマンドは、実行処理部 15 に、デジタルコンテンツの送信前における送信側 IC カード内各部の状態を記憶させ、デジタルコンテンツの送信後、送信先が受信処理を完了した旨を通知するコミット命令を受信した場合に、ホルダー部 18 内に格納されたデジタルコンテンツを消去する。デジタルコンテンツの送信処理の実行中に、通信が中断された場合には、実行処理部 15 に記憶された状態を読み出し、ロールバック処理によって各部を送信処理開始前の状態に復帰させる。

【0051】

一方、前記コマンドは、送信先 IC カードの実行処理部に対して、デジタルコンテンツの送信前における送信先 IC カード内部の状態を記憶させ、デジタルコンテンツの送信処理が中断された場合に、送信先の状態を記憶された状態に復帰させる。

【0052】

(データ交換システムを用いたデータ交換方法)

上述した構成を有する本実施形態に係るデータ交換システムを用いたデータ交換方法は、以下の手順による。図 3 は、本実施形態に係るデータ交換方法の全体

処理を示すシーケンス図であり、図4乃至図8は、本実施形態に係るデータ交換方法の手順を示すフロー図である。なお、ここでは、第1のICカード1aの操作者による操作に基づいて、第2のICカード1bとの交換処理が開始される場合を例に説明する。

### 【0053】

#### (1)全体処理

図3に示すように、全体処理としては、第1端末装置と第2端末装置との間で相互認証を行い（図中①）、相互認証が完了した後に、デジタルコンテンツの交換を行い（図中②）、両端末装置において受信が完了したのを確認することにより（図中③）、処理が終了する（図中④）。

### 【0054】

このとき、前提として、各ICカード1a及び1b内には既にデジタルコンテンツが格納されているものとする。すなわち、図4に示すように、デジタルコンテンツの提供者によりデジタルコンテンツ及び証明書データが発行され（S101）、それぞれを第1のICカード1a及び第2のICカード1b内のホルダー部18及び証明書データ格納部17に格納する（S102）。証明書データには、格納先であるICカード1aを識別するホルダーIDと、格納されたデジタルコンテンツに対応付けられた公開鍵、及び提供者によるデジタルコンテンツが正当である旨を証明するための署名データとが含まれている。

### 【0055】

そして、端末装置2aの操作者により、デジタルコンテンツの交換操作が開始される。具体的には、操作部24において交換開始の操作を行い、この操作に応じて、制御部26は、データ送受信部23及び12を通じてICカード1aにトリガー信号を出力する（S103）。

### 【0056】

このトリガー信号に応じて、実行処理部15は、コマンド記憶部16からコマンドを読み出し、交換処理を開始する。すなわち、認証処理（S104）を行った後、デジタルコンテンツの暗号化処理を行い（S105）、暗号化されたデジタルコンテンツを通信部21を通じて、第2のICカード1bに送信する（S1

06)。

#### 【0057】

このデジタルコンテンツを送信している間、通信監視部22は、送信状態を監視し(S107)、送信処理が中断されないか否かを判断し(S108)、交換処理が正常に完了した場合は(S109)、交換処理を完了し、ホルダー部18内のデジタルコンテンツを消去し、交換処理が正常に完了しなかった場合は、復帰処理(S110)を行う。

#### 【0058】

##### (2)認証処理

上述したステップS104における認証処理は、以下のように行われる。図4及び図5は、認証時の動作を示すフロー図である。

#### 【0059】

まず、第1の端末装置2aにおいては、認証処理が開始されると、証明書データ格納部17内の証明書データを第2の端末装置2bに送信する(S201)。この証明書データを受信した第2の端末装置2bは、受信した証明所内の署名データ及びホルダーIDに基づいて認証確認を行い、第1のICカード1aの正当性が確認された場合には、認証確認通知を、第1のICカード1aに対して送信する(S202、S203)。一方、送信元のICカード1aの正当性が否認された場合には、処理を中断する。ステップS203において送信された認証確認通知が、第1のICカード1aにおいて受信された場合には(S204)認証処理は終了する。

#### 【0060】

この第2のICカード1b側における認証処理と並行して、第1のICカード1a側においても認証処理が実行される。すなわち、第2のICカード1b側の認証部13は、第2のICカード1bから証明書データを取得し(S205)、取得した証明所内の署名データ及びホルダーIDに基づいて認証処理を行う(S206)。

#### 【0061】

そして、このようにして相互認証が完了した後、実行処理部15は、コマンド

記憶部16に記憶されたコマンドを呼び出し、交換処理を実行する。なお、本実施形態では、この相互認証時に、当該セッションでのみ有効なセッションIDを設定するとともに、セッションモードを相互に取得し(S207)、このセッションモードとICカードのカードIDに基づいてアクセスレベルを設定する(S208)。

#### 【0062】

このアクセスレベルに応じて、ホルダー部内のコンテンツのセキュリティレベルが決定され、このレベルに応じて、操作者に開示するコンテンツの内容が制限される。この開示制限が解除された情報については、ホルダー部18内から読み出しが可能となり、表示部25に表示される。この表示される情報としては、データのファイル名や内容の種類(電子マネーやクーポン・チケットなど)等が考えられる。

#### 【0063】

##### (3)交換処理

上述したステップS106における送信処理は、以下のように行われる。図6は、交換時の動作を示すフロー図である。

#### 【0064】

まず、交換処理が開始されると第1及び第2のICカード1a, 1bにおいて、処理開始時の状態を記憶する(S301及びS302)。次いで、第1の端末装置側からデジタルコンテンツの送信を行う(S303)。このとき、暗号化処理は完了しているものとする。

#### 【0065】

そして、第2のICカード1bにおいて受信が完了すると(S304)、ICカード1bの実行処理部15は、受信が正常に完了した旨を通知するコミット命令を、第1のICカード1aに対して送信する(S305)。

#### 【0066】

第1のICカード1a側でコミット命令が受信されたと判断されると(S306)、第1ICカード側の実行処理部15は、第2のICカード側に対して、デジタルコンテンツの送信を要求する。この要求を受けて第2のICカード側から

デジタルコンテンツの送信を行う（S307）。

【0067】

そして、第1のICカード1a側でデジタルコンテンツの受信が完了すると、第1のICカード1aからコミット命令を、第2のICカード1b側に送信する（S308）。第2のICカード1b側では、このコミット命令が受信されたか否かの判断を行い（S309）、コミット命令が受信された場合には、第1及び第2のICカード両者において、ホルダー部18内のデジタルコンテンツを消去する（S310）。

【0068】

一方、ステップS306又はS309においてコミット命令が受信されないと判断されると、第1のICカード1aは、送信が完了しているデジタルコンテンツの消去を行わず、記憶していた送信開始時の状態に復帰させ、一時的に保持した第2のICカードから送られてきたデジタルコンテンツを消去する（S311）。

【0069】

また、受信側のICカード1bにおいても、送信処理が中断されことなく終了した場合は、受信したデジタルコンテンツを保存し、処理を終了する。一方、ステップS306若しくはS309において送信処理の中断が生じた場合には、第2のICカード1bの状態を、送信開始時の状態に復帰させる（S503）。このとき、一時的に受信されていたデジタルコンテンツは消去され、第2のICカード側から送信したデジタルコンテンツの消去は行われない。

【0070】

(4)監視処理

上述した交換処理時には、上記ステップS107で示した通信状態の監視が行われる。図7は、この監視処理の動作を示すフロー図である。

【0071】

まず、送信されるコンテンツデータは、暗号化された後パケット化されて送信される。そして、各パケットの送信時を計測し、最後にデータを送信した時点を記憶する（S401）。そして、その最後にデータを送信した時点からの経過時



間を測定し、所定長の待機時間が経過する間に、送信先からなんらかの応答があるか否かを判断を行う（S402～S404）。

#### 【0072】

ステップS404において、送信先からの応答があった場合は、継続して経過時間の測定を行う（S402）。一方、ステップS405において、送信先からの応答が無かったと判断された場合には、中断処理を行う（S405）。この中断処理としては上述した各ICカードの復帰処理（S110）がある。

#### 【0073】

##### [第2実施形態]

##### (基本構成)

次いで、本発明の第2実施形態について説明する。本実施形態では、上述した第1実施形態で説明したデジタルコンテンツの交換システムを、チケットやクーポンを、電子マネーと交換することにより購入する電子商取引に应用することを特徴とする。

#### 【0074】

すなわち、上述した第1のICカードを、チケット等のデジタルコンテンツを発行し送信するコンテンツ発行サーバとし、発行したデジタルコンテンツをコンテンツ発行サーバから第2のICカードに送信する。第2のICカードは、購入したデジタルコンテンツの代金として電子マネーを支払う。図8乃至図10は、第2実施形態に係るデジタルコンテンツ発行システムの構成を模式的に示す説明図である。

#### 【0075】

図8に示すように、デジタルコンテンツ発行システムは、受信側ICカード1bに対してデジタルコンテンツの生成及び発行を行うコンテンツ発行サーバ11と、デジタルコンテンツの発行に用いられるcreateコマンド及びcreate権を生成・管理するコマンド生成サーバ3とを備える。

#### 【0076】

デジタルコンテンツの発行は、コンテンツ発行サーバ11で生成されたコンテンツを、ユーザーの有するICカード1b内に送信し、この送信したコンテンツ

と、電子マネーとを交換することにより行われる。

【0077】

詳述すると、コンテンツ発行サーバ11内に装填されたICカード1a内に一時的にデジタルコンテンツ（チケット等）を格納し、それをさらに第2のICカード1bに転送するとともに、第2のICカード1bから電子マネーを受信する。ICカード1aへのコンテンツの転送は、コマンド生成サーバ3から取得したcreateコマンドを実行することにより行い、このcreateコマンドを実行するには、コマンド生成サーバ3で発行されたcreate権が必要となる。

【0078】

コンテンツ発行サーバ11は、一時的にデジタルコンテンツを格納するICカード1aが装填されるインターフェースを備えており、デジタルコンテンツをcreateコマンドを用いて、ICカード1a内に転送するサービスを行うサーバである。

【0079】

このcreateコマンドは、図9に示すようにコンテンツ発行サーバ11からコマンド生成サーバ3に対して登録要求を送り、登録が認められたサーバに対して発行される実行プログラムであり、図10に示すように、実行される度に、コマンド生成サーバ3に認証要求を行い、当該コマンドに対するcreate権が存在するかを照合し、create権が発行されている場合にのみ動作し、create権が発行されていない場合には、動作を拒否する。

【0080】

なお、本実施形態におけるコマンド生成サーバ3における認証結果は、図10に示すように、コマンド生成サーバ3から送信されるackにより、コンテンツ発行サーバ11において確認される。すなわち、コンテンツ発行サーバ11では、デジタルコンテンツの生成時に、createコマンドを実行することにより、コマンド生成要求を送信し、これに対してコマンド生成サーバ3から送信されるackを取得し、デジタルコンテンツを生成する。

【0081】

コンテンツ発行サーバ11は、コンテンツを生成する際、コマンド生成サーバ

3へ登録を行い、createコマンドを取得する。この登録に基づいて、コマンド生成サーバ3では、当該createコマンドに対するcreate権を発行する。この発行されたcreate権は、登録サーバ管理データベースにおいて管理される。

#### 【0082】

コンテンツ発行サーバ11は、デジタルコンテンツの生成時に際し、コマンド生成サーバ3との間で認証を行い、create権を取得する。この認証では、コンテンツ発行サーバ11は、コマンド生成サーバ3へ、デジタルコンテンツ生成要求、個人（サーバ）情報、及びコンテンツ発行サーバ11自身の署名を送信する。

#### 【0083】

コマンド生成サーバ3は、createコマンドを生成（発行）し、コンテンツ発行サーバ11に対して送信するとともに、発行されたcreateコマンドに対応するcreate権を発行し、管理する管理サーバである。この管理には、登録サーバデータベース31に格納された登録サーバリスト31aが用いられる。

#### 【0084】

まず、コンテンツ生成要求と情報を受けたコマンド生成サーバ3は、サーバ情報からサーバの正当性を検証し、コンテンツ発行サーバ11が、デジタルコンテンツを生成する資格があると判断した場合は、登録サーバリスト31aに、当該コンテンツ発行サーバ11のサーバ名、及び個人情報を登録し、createコマンドをコンテンツ発行サーバ11へ送信する。

#### 【0085】

コマンド生成サーバ3では、コンテンツ発行サーバ11でデジタルコンテンツを生成する際、当該コンテンツ発行サーバ11から送信されたコンテンツ生成要求について登録サーバリスト31aの照合を行い、認証されたコンテンツ発行サーバのみにackを返す。

#### 【0086】

（動作）

上記構成を有するデジタルコンテンツ発行システムを用いたデジタルコンテンツの発行方法について説明する。図11は、本実施形態に係るデジタルコンテンツの発行方法を示すシーケンス図である。

## 【0087】

同図に示すように、先ず、コンテンツ発行サーバ11から、登録要求を送信する(S1101)。この登録要求と情報を受けたコマンド生成サーバ3は、サーバ情報からサーバの正当性を検証し、コンテンツ発行サーバ11が、デジタルコンテンツを生成する資格があると判断した場合は、登録サーバリスト31aに、当該コンテンツ発行サーバ11のサーバ名、及び個人情報を登録し(S1202)、createコマンドをコンテンツ発行サーバ11へ送信する(S1103)。

## 【0088】

次いで、コンテンツ発行サーバ11において、createコマンドが実行されると(S1104)、createコマンドは、コマンド生成サーバ3に対して、デジタルコンテンツ生成要求、個人(サーバ)情報、及びコンテンツ発行サーバ11自身の署名を送信する(S1105)。

## 【0089】

コマンド生成サーバ3では、当該コマンドに対するcreate権が存在するかを登録サーバリスト31aにおいて照合する(S1106)。このコマンド生成サーバ3における照合結果は、コマンド生成サーバ3から送信されるackとして、コンテンツ発行サーバ11に送信される(S1107)。

## 【0090】

コンテンツ発行サーバ11では、コマンド生成サーバ3から送信されるackを取得し、ackの内容が"OK"の場合は、デジタルコンテンツを生成し(S1108)、ackの内容が"reject"の場合は、デジタルコンテンツの生成を行わず、エラー処理を行う(S1109)。

## 【0091】

(変更例1)

なお、上述した第2実施形態は、以下のような変更を採用することができる。図12及び図13は、変更例1に係るデジタルコンテンツ発行システムの構成を示すブロック図である。本実施形態では、createコマンドとともに、create権自体をコンテンツ発行サーバ11へ発行する。

## 【0092】

図12及び図13に示すように、デジタルコンテンツ発行システムは、ICカード1aに対してデジタルコンテンツの生成及び発行を行うコンテンツ発行サーバ11と、デジタルコンテンツの発行に用いられるcreateコマンド及びcreate権を生成・管理するコマンド生成サーバ3'とを備える。本実施形態に係るコマンド生成サーバ3'は、createコマンドとcreate権とを対応付けて送信する発行権管理手段32を有する。

#### 【0093】

コンテンツ発行サーバ11は、コマンド生成サーバ3'から受信したcreateコマンド及びcreate権をICカード1a内に格納する。createコマンドは、実行される度に、ICカード1a内において、当該createコマンドに対応付けられて格納されているcreate権を確認し、create権が存在する場合には、デジタルコンテンツを生成し、存在しない場合にはエラー処理を行う。

#### 【0094】

上記構成を有するデジタルコンテンツ発行システムの動作について説明する。図14は、本実施形態に係るデジタルコンテンツの発行方法を示すシーケンス図である。

#### 【0095】

まず、コンテンツ発行サーバ11からコマンド生成サーバ3'に対して、コンテンツ生成要求、及び個人情報を送信する(S1201)。この送信に応じて、コマンド生成サーバ3'は、受信した個人情報を検証し、コンテンツ発行サーバ11に、デジタルコンテンツを生成する資格があるか否かを検証し(S1202)、資格があると判断した場合には、コンテンツ発行サーバ11に対し、create権及びcreateコマンドを送信する(S1203)。この送信されたcreate権及びcreateコマンドは、コンテンツ発行サーバ11内のICカード1a内に直接格納される(S1204)。

#### 【0096】

そして、コンテンツ発行サーバ11がデジタルコンテンツを生成する場合は、createコマンドを実行する(S1205)。この際、createコマンドは、ICカード1a内のcreate権が存在するか否かを確認する(S1206)。ICカード

1 a内にcreate権が存在すれば、生成サーバはcreateコマンドを用いて、デジタルコンテンツを生成し（S 1 2 0.7）、存在しない場合には、エラー処理を行う。

#### 【0097】

##### （変更例2）

上記第2実施形態の他の変更例について説明する。図15及び図16は、変更例2に係るデジタルコンテンツ発行システムの構成を示すブロック図である。本実施形態では、生成サーバの正当性の検証を、ソフトウェアではなく、物理的に行う。

#### 【0098】

図15及び図16に示すように、本実施形態に係るデジタルコンテンツ発行システムは、ICカード1aに対してデジタルコンテンツの生成及び発行を行うコンテンツ発行サーバ11を設け、このコンテンツ発行サーバ11は、最初からcreateコマンドが焼き込まれたICカード（チップ）4が接続されており、デジタルコンテンツを生成する際には、このコマンド内蔵ICカード4にアクセスしcreateコマンドを呼び出し、実行する。

#### 【0099】

コマンド内蔵ICカード4は、createコマンドが物理的に固定されており、外部からの変更ができないようになっている。システムを変更する場合には、物理的にチップを変更することでサーバを変更する。

#### 【0100】

##### （変更例3）

次いで、変更例3について説明する。図17及び図18は、変更例3に係るデジタルコンテンツ発行システムの構成を示すブロック図である。本実施形態では、正しく認証されたコンテンツ発行サーバのIDを用いてcreateコマンドを暗号化して当該コンテンツ発行サーバ11に対して送信する。

#### 【0101】

図17及び図18に示すように、本実施形態に係るデジタルコンテンツ発行システムは、ICカード1aに対してデジタルコンテンツの生成及び発行を行うコ

ンテンツ発行サーバ11と、デジタルコンテンツの発行に用いられるcreateコマンドを生成するコマンド生成サーバ3”とを備える。本実施形態に係るコマンド生成サーバ3”は、正しく認証されたコンテンツ発行サーバのIDを用いてcreateコマンドを暗号化して当該コンテンツ発行サーバ11に対して送信する機能を有する。

#### 【0102】

すなわち、コマンド生成サーバ3”は、コンテンツ発行サーバ11からデジタルコンテンツ生成要求、及び個人情報（コマンド生成サーバのIDを含む）を取得し、この個人情報に基づいて認証を行った後、デジタルコンテンツを生成する資格があると判断した場合には、コマンド生成サーバのIDを用いてcreateコマンドを暗号化し、コンテンツ発行サーバ11へ送信する。

#### 【0103】

一方、コンテンツ発行サーバ11はこの暗号化されコマンドを受け取り、ICカード1a内に直接格納する。ICカード1a内では、サーバの個人情報からIDを抽出し、createコマンドの復号を行い、復号されたcreateコマンドを実行し、コンテンツを生成する。

#### 【0104】

すなわち、図13に示すように、コマンド生成サーバ3”は、コンテンツ発行サーバ11からデジタルコンテンツ生成要求、及び個人情報（コマンド生成サーバのIDを含む）を取得し（S1301）、この個人情報に基づいて認証を行った後（S1302）、デジタルコンテンツを生成する資格があると判断した場合には、コマンド生成サーバのIDを用いてcreateコマンドを暗号化し（S1303）、コンテンツ発行サーバ11へ送信する（S1304）。

#### 【0105】

一方、コンテンツ発行サーバ11はこの暗号化されコマンドを受け取り、ICカード2内に直接格納する。ICカード2内では、サーバの個人情報からIDを抽出し、createコマンドの復号を行い（S1305）、復号されたcreateコマンドを実行し、コンテンツを生成する（S1306）。

#### 【0106】

これにより、正しく認証されたサーバのみにcreateコマンドを送付することが可能となる。

#### 【0107】

##### 【発明の効果】

以上説明したように本発明によれば、外部の端末装置やサーバのコマンドを用いることなく、ICカード内部に備えられたアトミックなコマンドを用いて暗号化や交換処理を行うことから、外部の端末装置やサーバ側からの不正な操作による影響を回避することができ、外部の装置のセキュリティー環境によらず、安全なデジタルコンテンツの送信を行うことができる。この結果本発明によれば、ICカード間で直接通信を行うプラットフォーム上で、デジタルコンテンツを交換する際に、送受信者及び悪意のある第三者による複製や紛失を回避することができる。

##### 【図面の簡単な説明】

#### 【図1】

第1実施形態に係るデータ交換システムの全体構成を示すブロック図である。

#### 【図2】

第1実施形態に係るデータ交換システムのICカード及び端末装置の内部構造を示すブロック図である。

#### 【図3】

第1実施形態に係るデータ交換システムの全体動作を示すシーケンス図である。

#### 【図4】

第1実施形態に係るデータ交換システムの全体動作を示すフロー図である。

#### 【図5】

第1実施形態に係るデータ交換システムの認証処理動作を示すフロー図である。

#### 【図6】

第1実施形態に係るデータ交換システムの交換処理動作を示すフロー図である。



**【図 7】**

第 1 実施形態に係るデータ交換システムの監視処理動作を示すフロー図である。

**【図 8】**

第 2 実施形態に係るデジタルコンテンツ発行システムの概要を示す説明図である。

**【図 9】**

第 2 実施形態に係るデジタルコンテンツ発行システムの概略構成を示す説明図である。

**【図 10】**

第 2 実施形態に係るデジタルコンテンツ発行システムの動作を示す説明図である。

**【図 11】**

第 2 実施形態に係るデジタルコンテンツ発行システムの動作を示すシーケンス図である。

**【図 12】**

第 2 実施形態の変更例 1 に係るデジタルコンテンツ発行システムの概要を示す説明図である。

**【図 13】**

上記変更例 1 に係るデジタルコンテンツ発行システムの概略構成を示す説明図である。

**【図 14】**

上記変更例 1 に係るデジタルコンテンツ発行システムの動作を示すシーケンス図である。

**【図 15】**

第 2 実施形態の変更例 2 に係るデジタルコンテンツ発行システムの概要を示す説明図である。

**【図 16】**

上記変更例 2 に係るデジタルコンテンツ発行システムの概略構成を示す説明図

である。

【図 17】

第2実施形態の変更例3に係るデジタルコンテンツ発行システムの概要を示す説明図である。

【図 18】

上記変更例3に係るデジタルコンテンツ発行システムの概略構成を示す説明図である。

【図 19】

上記変更例3に係るデジタルコンテンツ発行システムの動作を示すシーケンス図である。

【符号の説明】

- 1 a…第1のICカード
- 1 b…第2のICカード
- 2…端末装置
- 3…コマンド生成サーバ
- 4…コマンド内蔵ICカード
- 11…コンテンツ発行サーバ
- 11 a, 11 b…ICチップ
- 12…データ送受信部
- 13…認証部
- 14…暗号処理部
- 15…実行処理部
- 16…コマンド記憶部
- 17…証明書データ格納部
- 18…ホルダー部
- 2 a…第1の端末装置
- 2 b…第2の端末装置
- 21…通信部
- 22…通信監視部

23, 12...データ送受信部

24...操作部

25...表示部

26...制御部

31...登録サーバデータベース

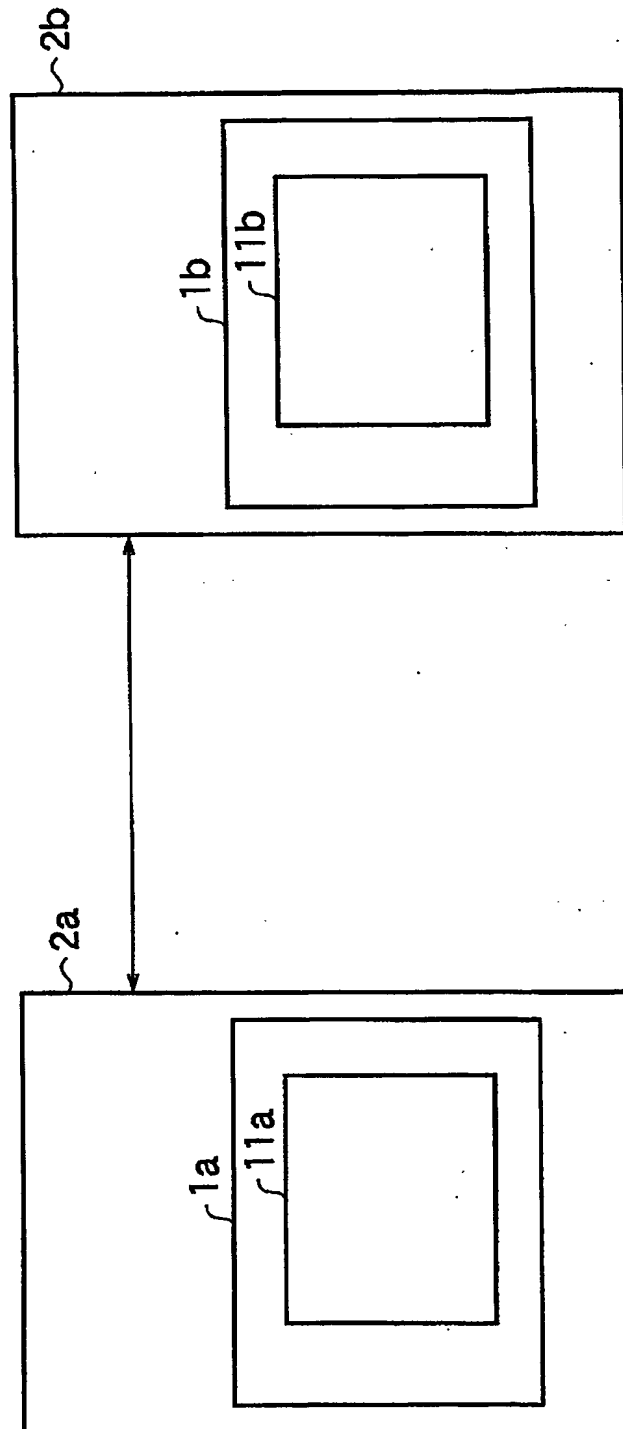
31a...登録サーバリスト

32...発行権管理手段

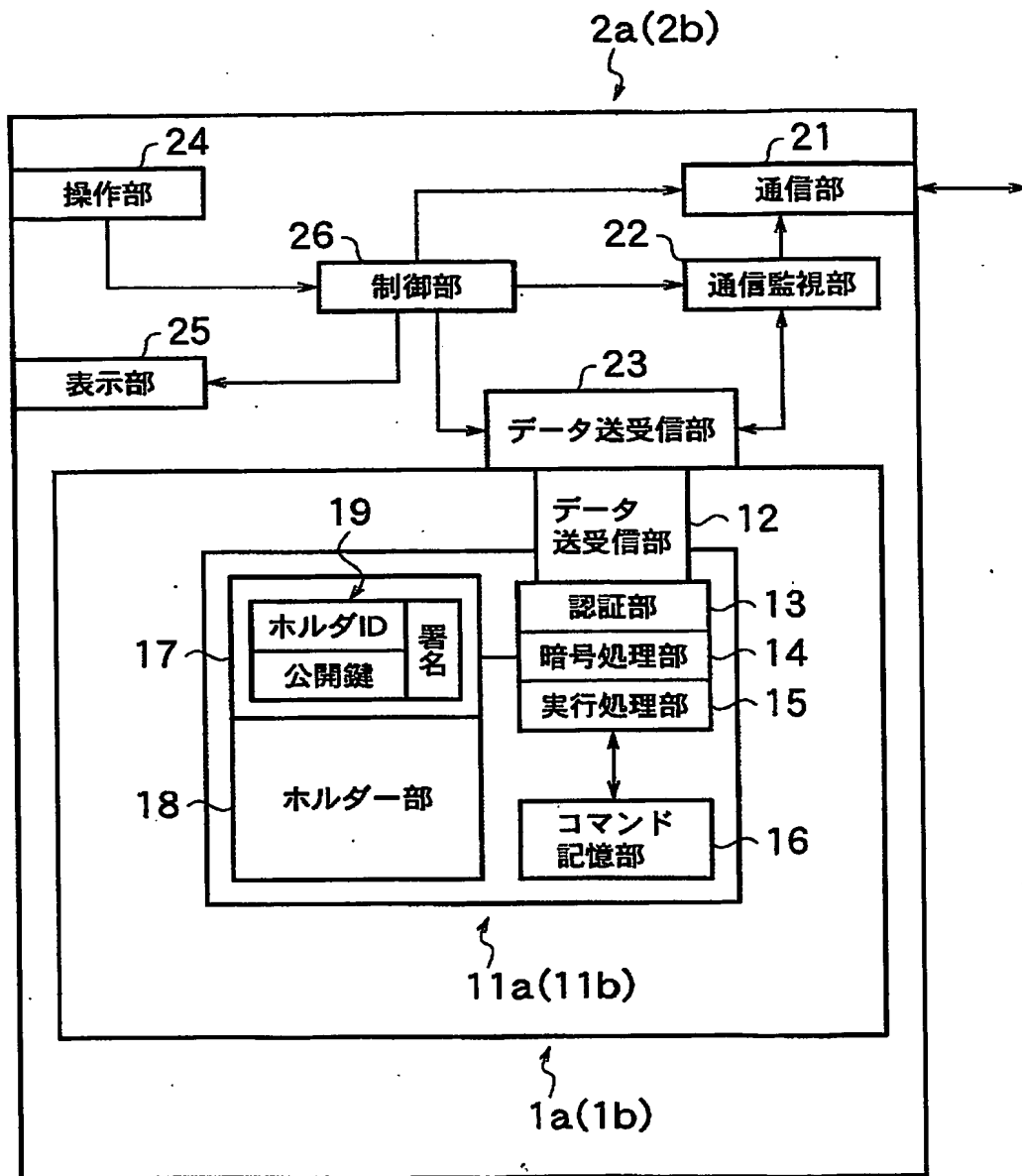
【書類名】

図面

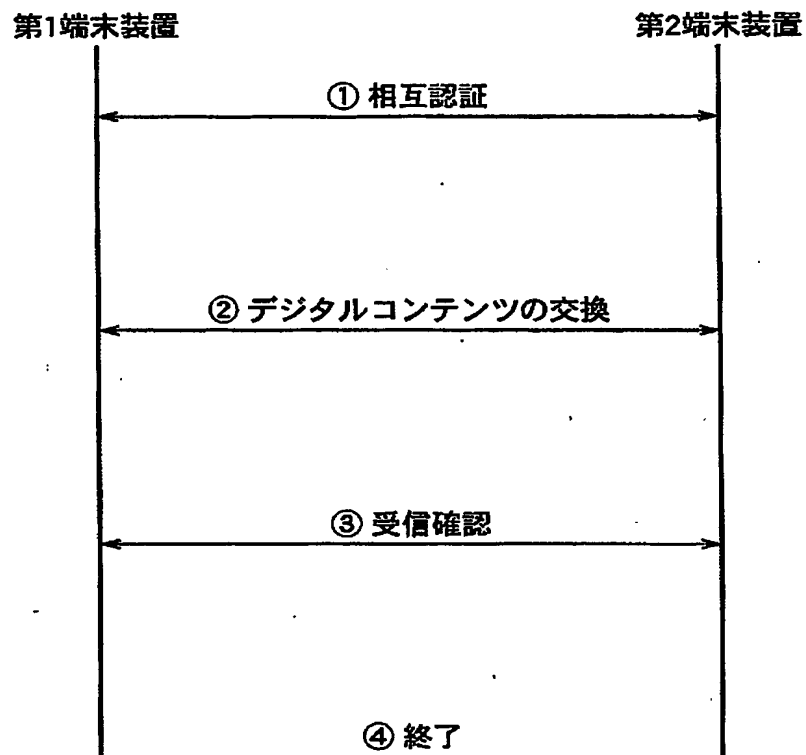
【図 1】



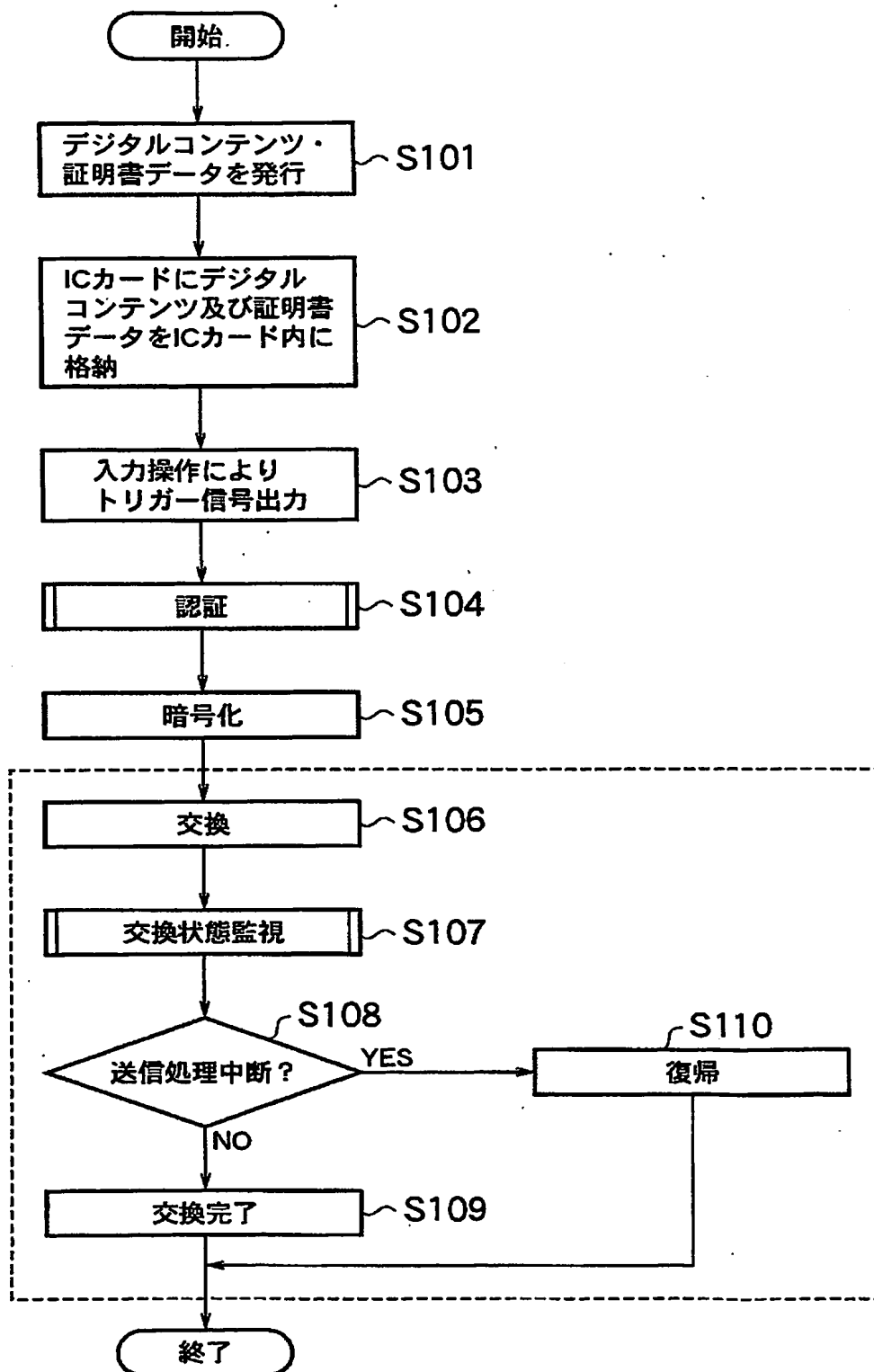
【図 2】



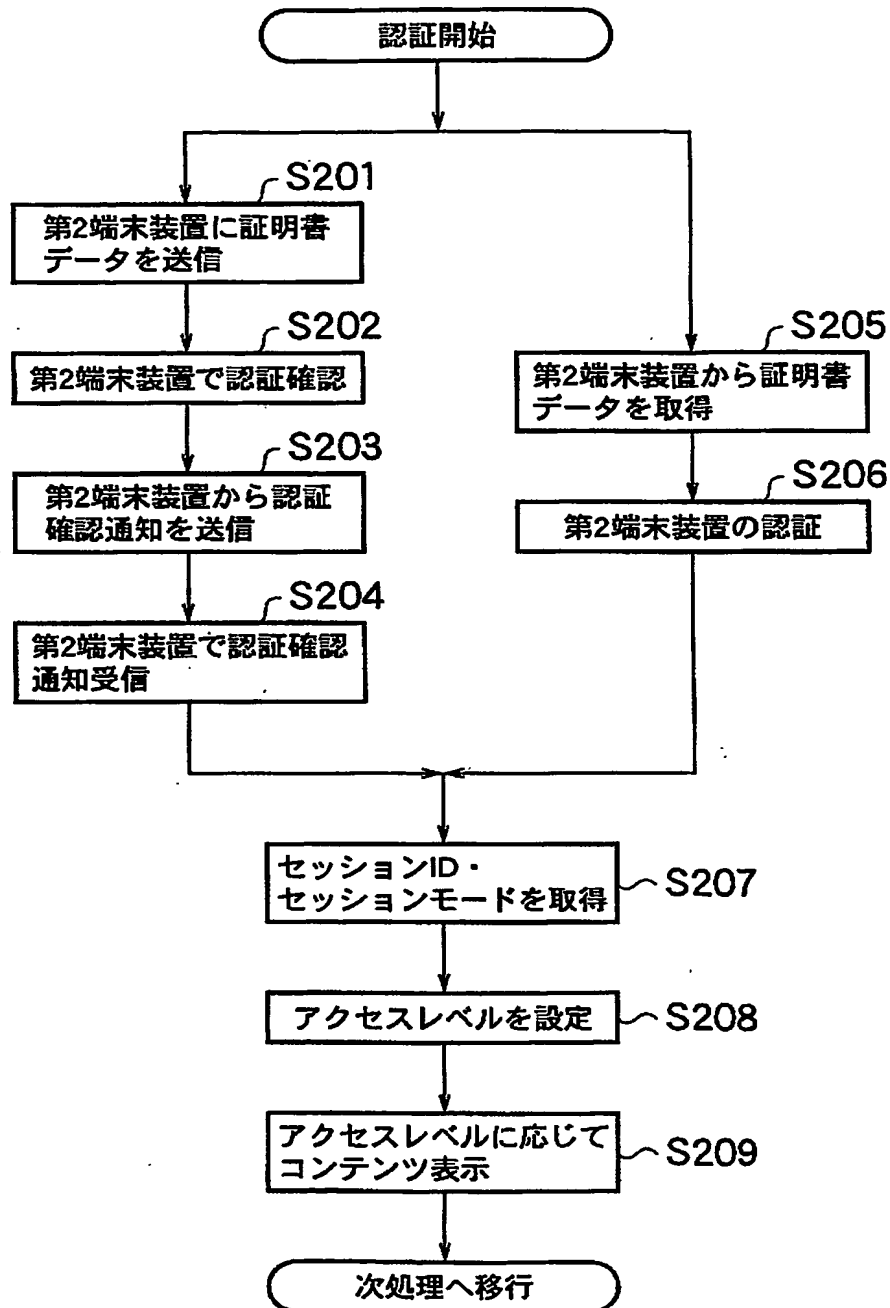
【図3】



【図 4】

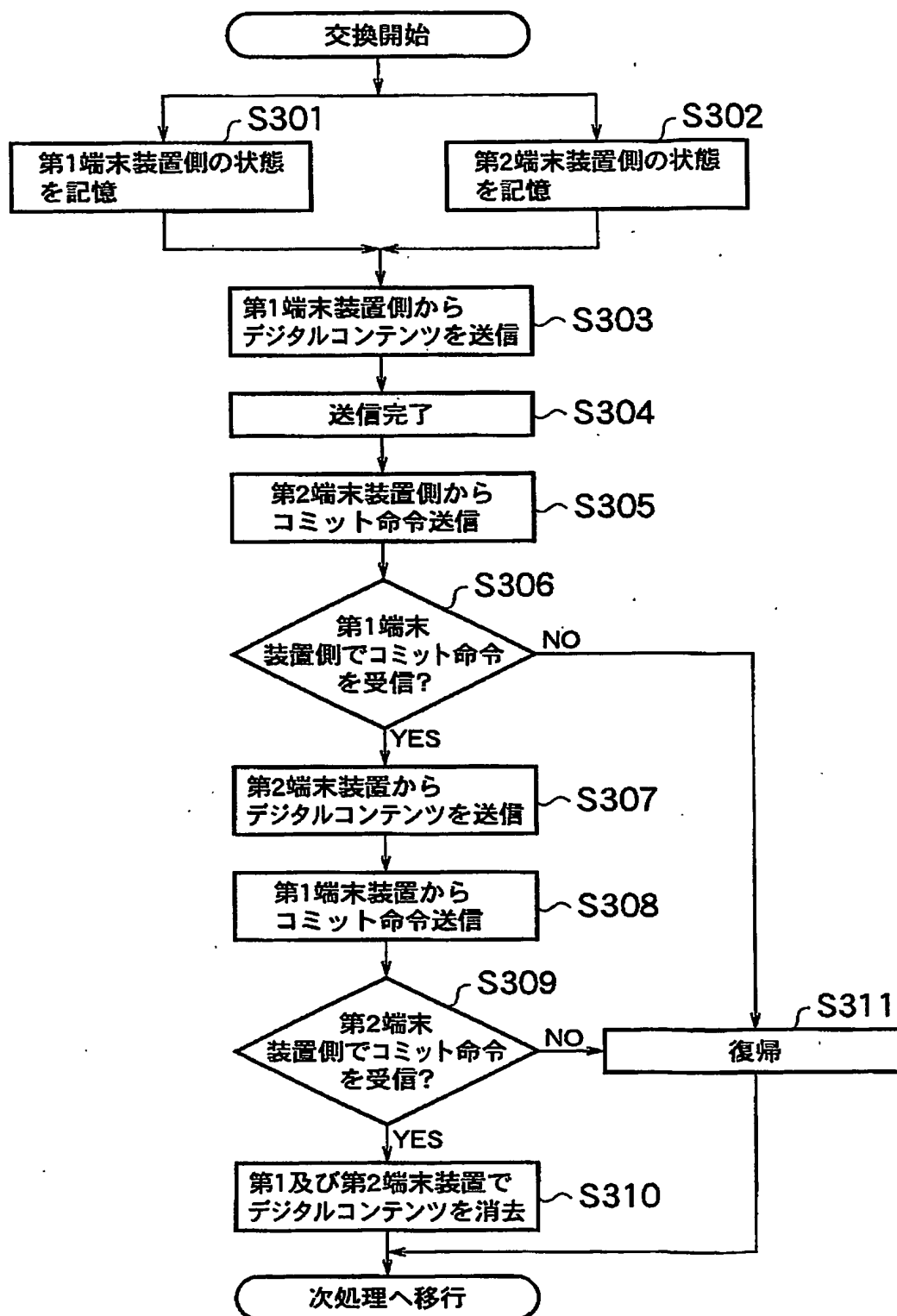


【図5】

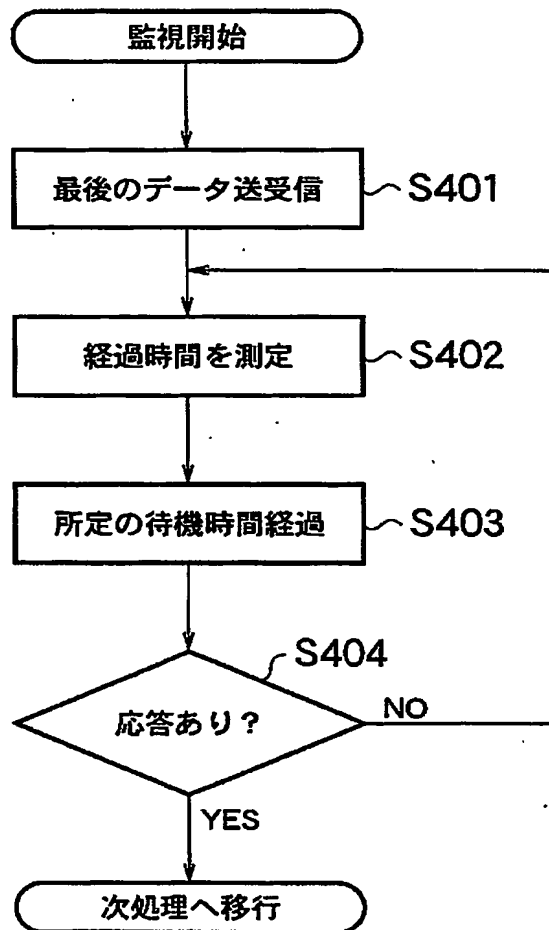




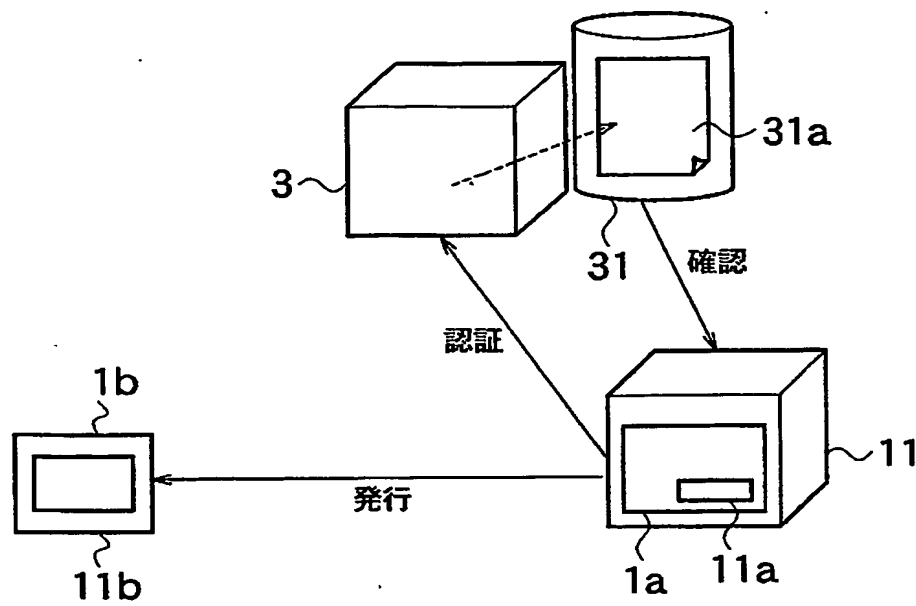
【図 6】



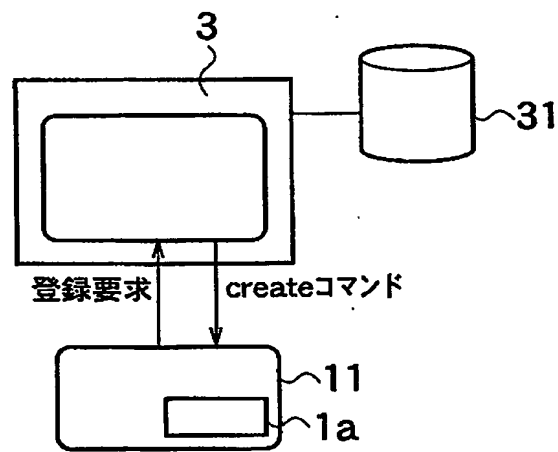
【図 7】



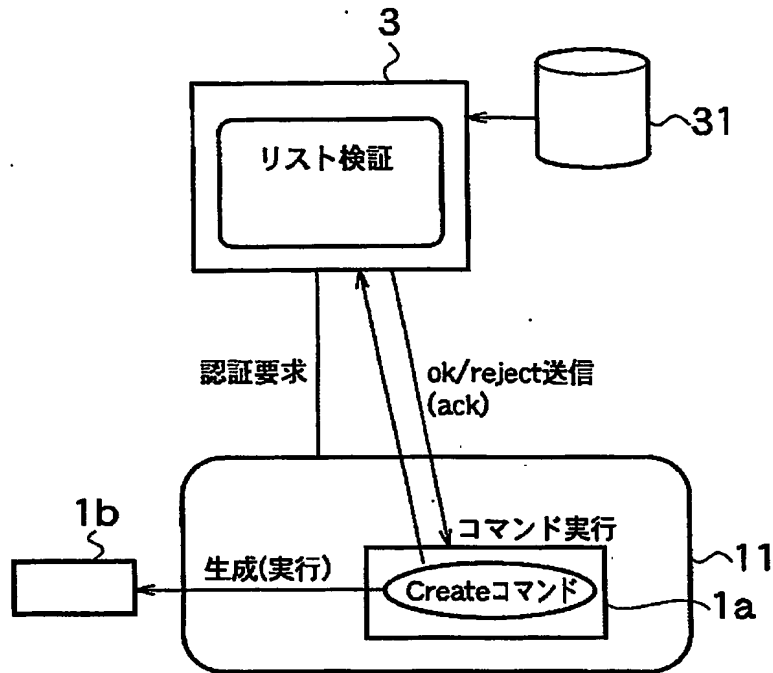
【図 8】



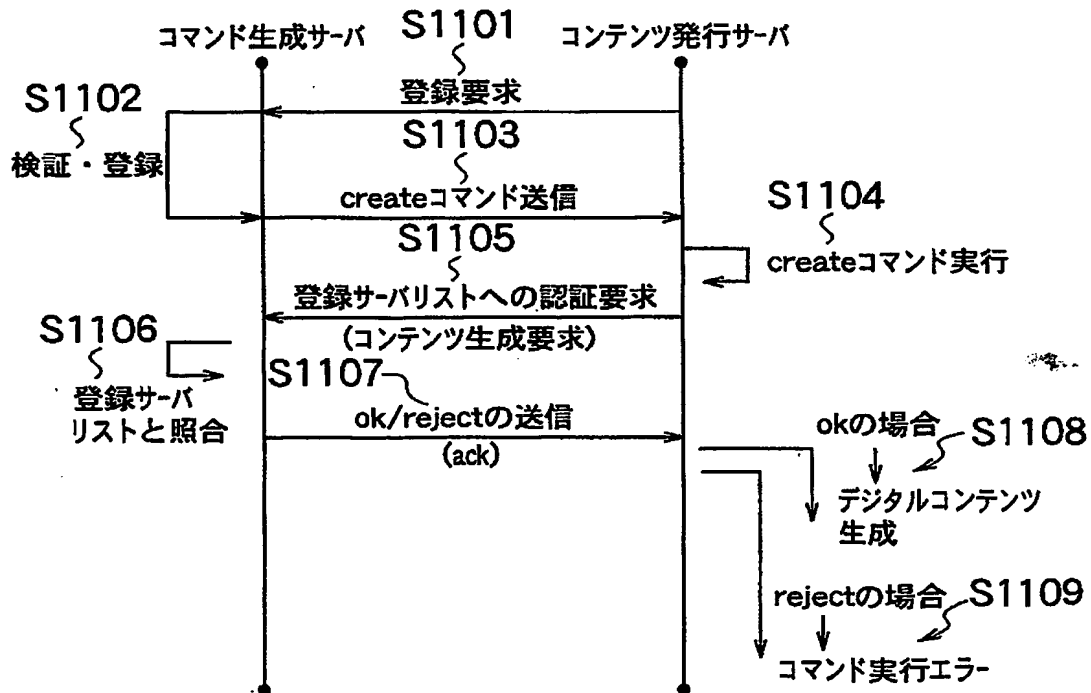
【図 9】



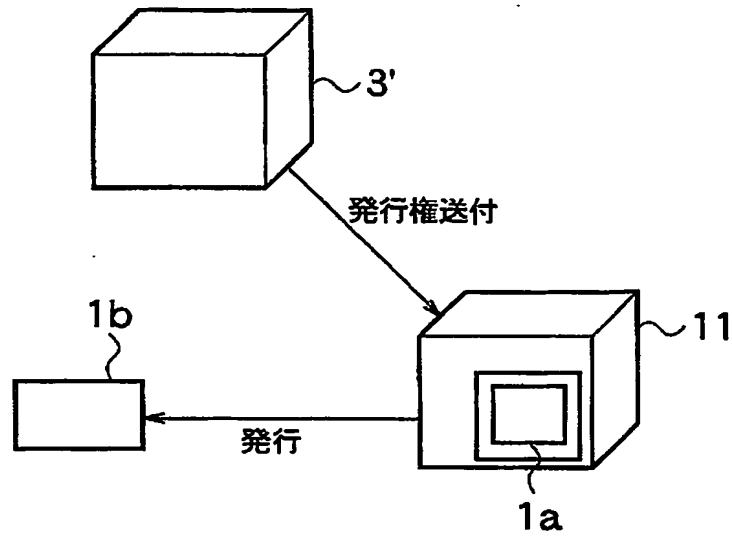
【図10】



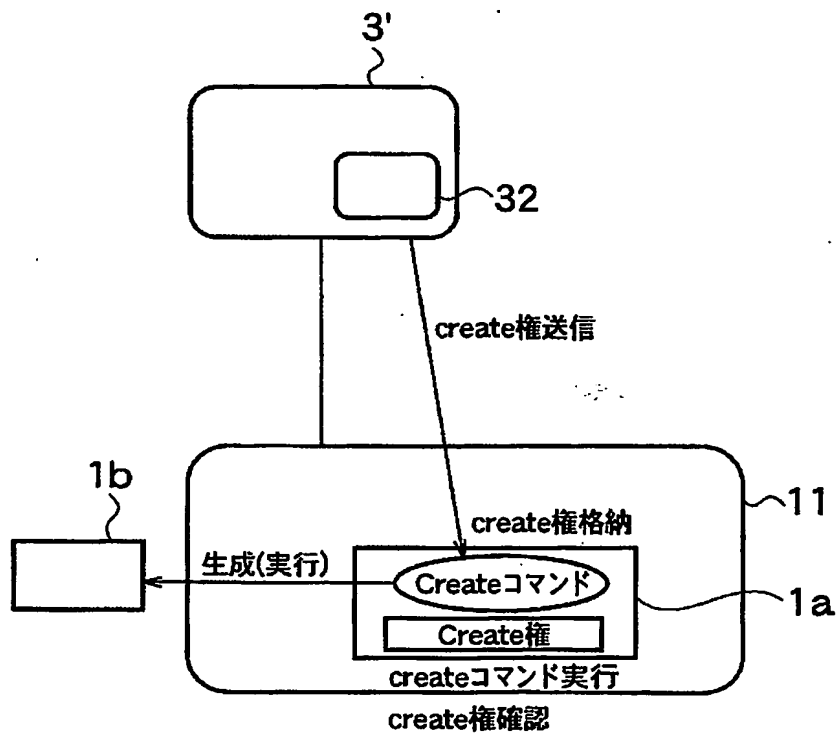
【図11】



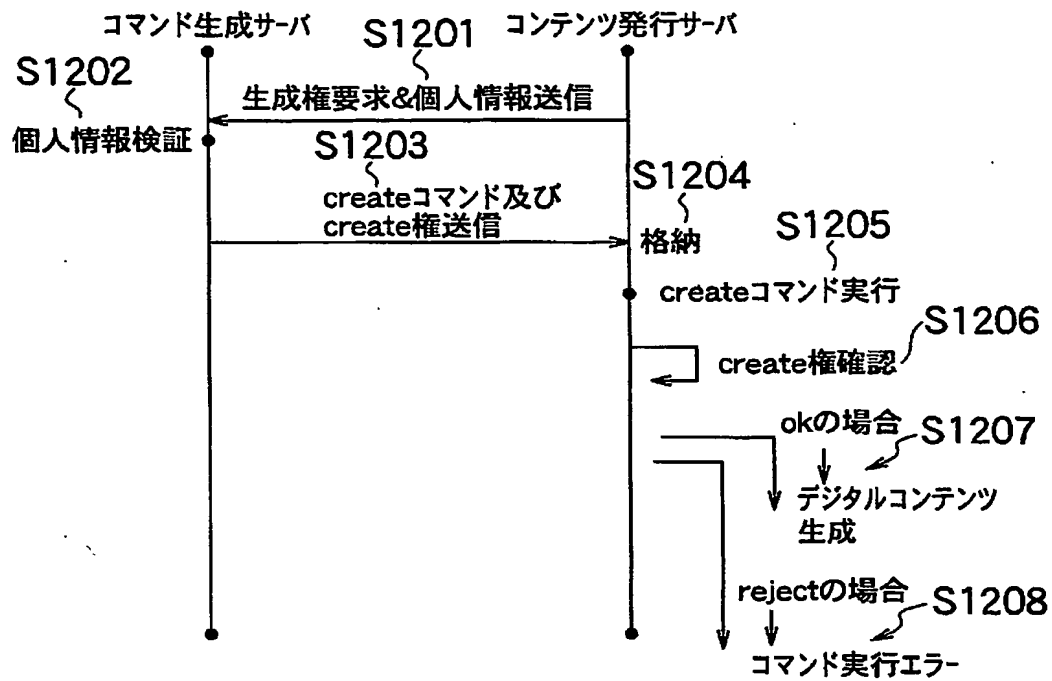
【図12】



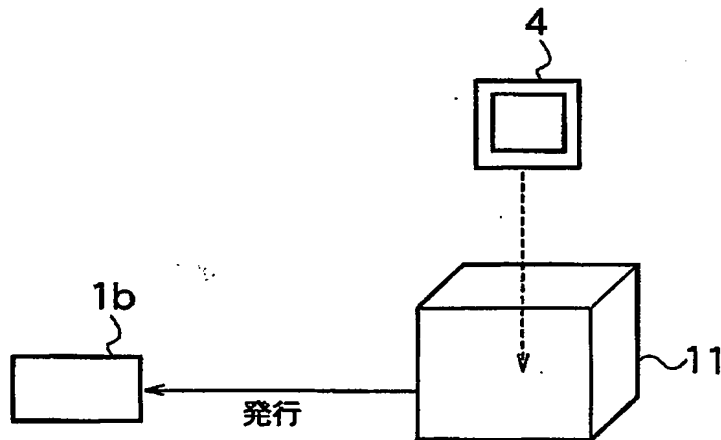
【図13】



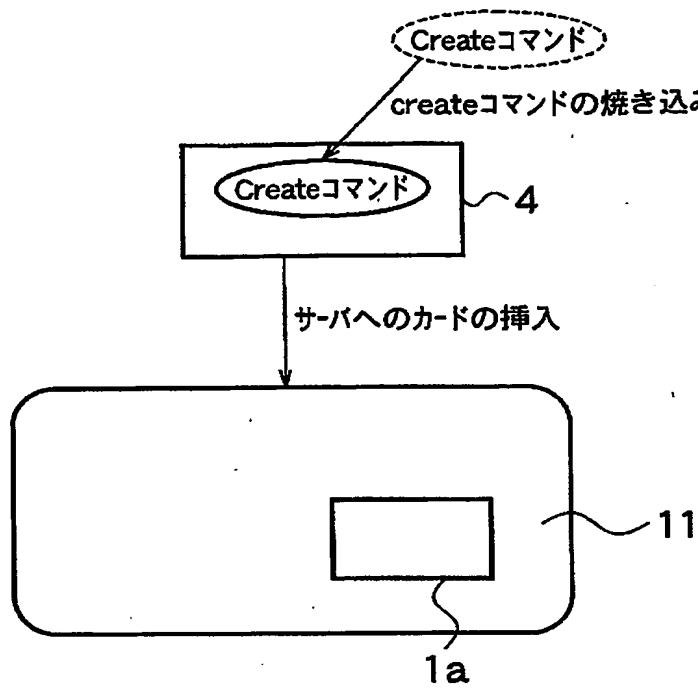
【図 14】



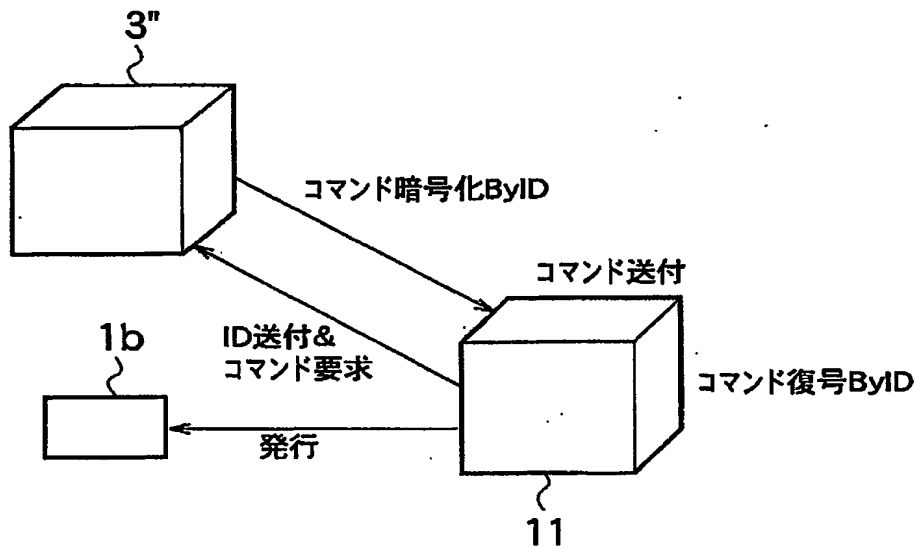
【図 15】



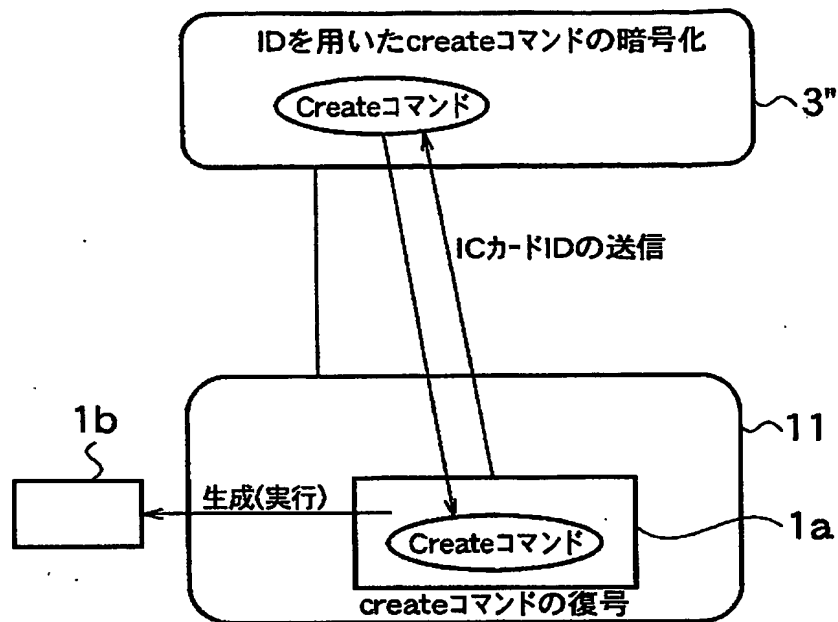
【図16】



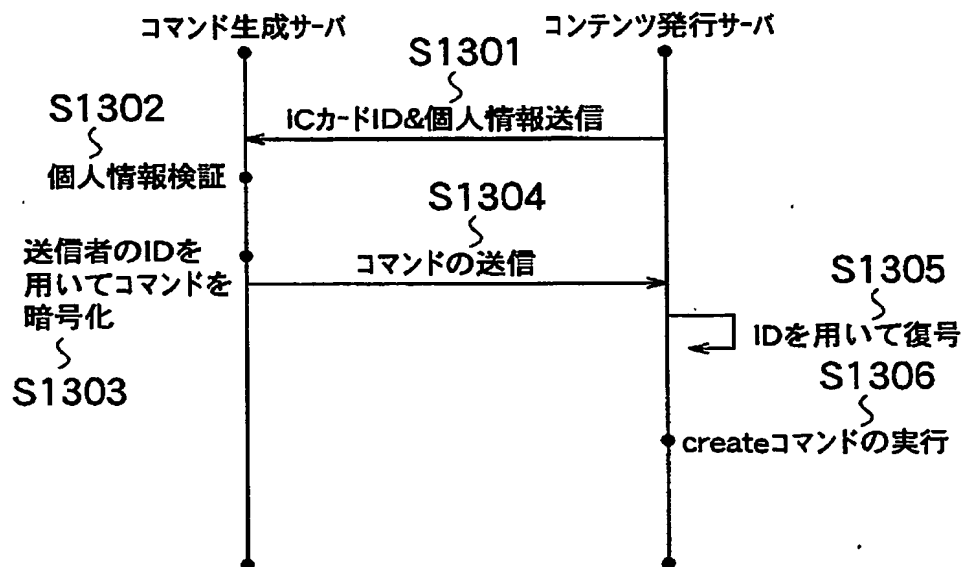
【図17】



【図18】



【図19】





【書類名】 要約書

【要約】

【課題】 ICカード間で直接通信を行うプラットフォーム上でデジタルコンテンツを交換する際に、送受信者及び悪意のある第三者による複製や紛失を回避する。

【解決手段】 ホルダー部に格納されたデジタルコンテンツに対応付けられた鍵情報を含む証明書データを格納する証明書記憶部と、格納されたデジタルコンテンツを鍵情報に基づいて暗号化する暗号処理部と、暗号化されたデジタルコンテンツを他の機器に対して送信するとともに、他の機器が保持するデジタルコンテンツを受信するデータ送受信部と、ホルダー部に格納されたデジタルコンテンツを暗号処理部により暗号化し、これをデータ送信部を通じて送信するとともに他の機器からデジタルコンテンツを受信するコマンドを記憶するコマンド記憶部と、トリガー信号に基づいてコマンドを実行する実行処理部とを備える。

【選択図】 図2

特願 2002-169241

出願人履歴情報

識別番号

[592146793]

1. 変更年月日

1992年 6月12日

[変更理由]

新規登録

住 所

東京都品川区大崎4-9-2

氏 名

坂村 健

特願 2002-169241

出 願 人 履 歴 情 報

識別番号

[392026693]

1. 変更年月日

1992年 8月21日

[変更理由]

新規登録

住 所

東京都港区虎ノ門二丁目10番1号

氏 名

エヌ・ティ・ティ移動通信網株式会社

2. 変更年月日

2000年 5月19日

[変更理由]

名称変更

住所変更

住 所

東京都千代田区永田町二丁目11番1号

氏 名

株式会社エヌ・ティ・ティ・ドコモ

特願2002-169241

出願人履歴情報

識別番号

[502180015]

1. 変更年月日

2002年 5月20日

[変更理由]

新規登録

住 所

東京都武蔵野市西久保2-27-20

氏 名

越塚 登